情報セキュリティ実施基準

第１章　総　　則

（目的）

第１条　この基準は、「個人情報の保護に関する法律」の趣旨に基づき、株式会社ジェイリック（以下「会社」という。）が取り扱う情報及び情報システムの適切な運用を図るために、役員、顧問、社員及び嘱託（以下「従業者」という。）が最低限遵守すべき事項を明らかにし、もって情報の漏えい、き損、滅失等の事故の防止、情報システムの適切な運用、及び万が一の事故の場合の損害を最低限にすることを目的とする。

第２章 情報の指定・解除

（情報の指定・解除）

第２条　会社が保有する情報のうち、漏えい等が発生した場合、会社に重大な損害を及ぼすおそれが高い情報を秘密情報として指定する。

２　秘密情報が記載された紙の文書を秘密文書といい、パソコンのハードディスク、USB メモリー等の電磁媒体に保存された状態の秘密情報を秘密デジタルデータ（秘密DD）という。

３　秘密情報を指定した者又は代表取締役は、その情報が秘密でなくなった場合には、秘密情報であることを解除することができる。

４　秘密文書には、秘密であることを表示する。秘密情報が解除された場合は、秘密の表示を消去又は取り消し線で消す。

５　秘密 DD はファイルを開けるために必要なパスワードを設定する。

（秘密保持の方法）

第３条　受領もしくは取得した秘密文書は、速やかにデジタルデータに変換し、同時にそのファイルを開くためのパスワードを設定して、指定されたファイルサーバーに保存する。

２　デジタルデータ化された秘密文書は即座にシュレッダー処理する。受領した秘密文書で返還の必要がある等シュレッダー処理できない場合は、即座に返還処理するか、第4 条に規定する秘密文書の取り扱いに従う。

３　秘密 DD の閲覧、編集、保存は、パスワード保護された指定パソコン等を用いる場

合を除きこれを認めない。
４　会社は従業者の秘密 DD の紙媒体への印刷、別名ファイル保存及び部分コピーを禁止する処置を講ずる。
５　秘密 DD を紙媒体にする必要が発生した場合は、秘密情報を指定した者又は代表取締役の許可を得て、秘密 DD を印刷し、その印刷物を秘密文書として取り扱うことができる。

第３章 秘密情報の取扱い

（保管）

第 4 条　秘密文書を保管する場合は、キャビネット等に保管し、施錠する。
２　前項については、USB メモリー、CD-ROM その他の携帯することが可能な電子媒体（以下、「携帯可能媒体」という。）に保存する場合も同じものとする。
３　秘密 DD を保管する場合は、パスワード保護された会社指定コンピュータ等のみがアクセスできる会社指定ファイルサーバーに保管する。

（作業上の注意点）

第 5 条　業務時間内に一時的に離席する場合、秘密文書を机上等に放置せず、机の引き出しその他目につかない場所に一時的に保管する。
２　業務時間内に一時的に離席する場合等、コンピュータ等から一時的に離れる場合は、コンピューター等をパスワード入力が必要なスリープモードにする。

（持ち出しの制限）

第 6 条　秘密文書、秘密情報を保管した携帯可能媒体又はコンピュータ等を社外に持ち出すときは、所属する部門責任者又は代表取締役の承認を得る。

（郵送、FAX、電子メールの制限）

第 7 条　秘密文書又は秘密情報を保管した携帯可能媒体を郵送する場合は、事前に部門責任者又は代表取締役の承認を得たうえで、書留等、受取が確実に行われたことがわかる通信手段により行う。
２　秘密文書を FAX で送信してはならない。
３　電子メールで秘密情報を送信する場合は、事前に部門責任者又は代表取締役の承認を得たうえで、暗号化又はパスワードによる保護をし、送信する。

（印刷・複写・複製の制限）

第 8 条　秘密文書を印刷、複写、複製する場合は、部門責任者又は代表取締役の承認を得る。

（廃棄・返却）

第 9 条　秘密文書の廃棄は、シュレッダーによるクロス裁断処理か溶解処理による。

２　携帯可能媒体を廃棄する場合は、専用ソフトによる上書消去、携帯可能媒体の細断、焼却、溶解等復元できない方法による。

３　コンピュータ等を廃棄又はリース会社への返却する場合は、廃棄又は返却する前に専用ソフトによる上書消去をする。この作業は、守秘義務契約を結んだ第三者に委託することができる。

第４章 認証及びアクセス管理

（ID の登録・休止・廃止）

第10条　会社のコンピュータ等を利用する場合、事前に利用者に対し ID を付与する。

２　ID を付与した者は、ID は適切に管理する。

３　ID を付与した者が長期休暇、休職等一ヶ月以上会社のコンピュータ等を利用することがないと想定される場合、速やかに ID の利用を停止する。

４　ID を付与した者が退職等によって会社のコンピュータ等を利用する必要がなくなった場合、速やかに ID の利用を停止する。

５　会社指定のファイルサーバーに関しても、前 1 項から 4 項までの「コンピューター等」の文言を「会社の秘密情報が保存されているファイルサーバー」に読み替えて準用する。

（パスワード等による認証）

第 11 条　会社のコンピュータ等及び会社指定ファイルサーバーを利用する者は、パスワードにより認証する。

（利用者のパスワード等の管理）

第 12 条　パスワードにより本人を認証する場合、コンピュータ等の利用者は、他人に推測されにくいパスワードをつけ、他人に漏れないように適切に管理する。

（アクセス権の管理）

第 13 条　秘密情報をコンピュータ等や会社指定ファイルサーバーに保存する場合、秘密情報を閲覧する権限がない者が閲覧できない状態となるようにアクセス権を設定する。

２　業務が変更になる等、アクセス権を付与していた者にアクセス権を付与する必要がなくなった場合は、速やかにアクセス権を剥奪する。

第５章 コンピュータの適正利用

（会社のコンピュータの利用の前提）

第 14 条　会社のコンピュータ等や会社指定ファイルサーバーを利用するに当たり、自らのコンピュータ等や会社指定ファイルサーバー利用状況が記録され、確認される可能性があることに同意した者のみに、会社のコンピュータ等や会社指定ファイルサーバーの利用を認める。

（私的利用の禁止）

第 15 条　会社のコンピュータ等や会社指定ファイルサーバー利用者は、担当部門業務の目的のみこれを利用し、私的な利用を禁止する。

２　会社のコンピュータ等利用者は、担当部門業務の目的のみに、電子メールを利用し、私的な利用を禁止する。

３　会社のコンピュータ等利用者は、担当部門業務の目的のみに、インターネットのホームページを閲覧し、私的な利用を禁止する。

４　代表取締役は、必要に応じ、不必要なインターネットホームページへのアクセスを制限するソフトを導入することができる。

５　代表取締役は、必要に応じ、会社コンピュータ等や会社指定ファイルサーバー利用者のコンピュータ利用状況を確認することができる。

６　代表取締役は、上記の確認の結果、第 1 項から第 3 項に違反している可能性があると判断した場合は、本人から事情を聴取し、違反があればコンピュータ等や会社指定ファイルサーバーの利用を停止することができる。

（ソフトウェアライセンスの管理）

第 16 条　総務責任者は、会社のコンピュータ等に標準的にインストールするソフトウェアを定め、ライセンスを適切に管理しなければならない。

（ソフトウェアの無断インストールの禁止）

第 17 条　会社のコンピュータ等利用者は、会社が認めたソフトウェアのみをインストールして利用し、ソフトウェアを無断でインストールしてはならない。

２　会社のコンピュータ等利用者は、業務上の必要性によりソフトウェアをインストールする必要が生じた場合、代表取締役又は総務責任者に承認を得、ソフトウェアをインストールしなければならない。

３　総務責任者は、無断でインストールしたソフトウェアを発見した場合、会社のコンピュータ等利用者に対し、そのソフトウェアを消去することを指示しなければならない。

（コンピュータウィルス対策ソフトの導入）

第 18 条　総務責任者は、会社で利用する全てのコンピュータ等にコンピュータウィルス対策ソフトをインストールしなければならない。

２　会社のコンピュータ等利用者は、コンピュータウィルス対策ソフトが起動している状態でコンピュータ等を利用しなければならない。

３　コンピュータウィルスのパターンファイル又はソフトウェアは、常に最新に保たれるように設定する。

（システム上の脆弱性の管理）

第 19 条　総務責任者は、会社で利用するコンピュータ等について、オペレーティングシステムのバグその他のシステム上の脆弱性の存在を知った場合、セキュリティパッチソフトの導入その他の対策を検討しなければならない。

第 20 条　会社のコンピュータ等利用者は、総務責任者の指示によりセキュリティパッチソフトの導入が指示された場合、速やかに導入を行わなければならない。

第 6 章 ネットワーク及びサーバの管理

（管理者の設置と役割）

第 21 条　会社のネットワーク機器、ファイルサーバ及びクライアントコンピュータについて、システム管理者を設置する。

２　システム管理者は、ネットワーク機器、ファイルサーバについての運用管理を行う。

（サーバの管理）

第 22 条　会社のファイルサーバのシステム管理者は、ファイルサーバに対するアクセス制御方針を定め、外部、内部からの無権限アクセスを防止する。この作業は、守秘義務契約を結んだ第三者に委託することができる。

（ネットワークの管理）

第 23 条　会社のネットワークと外部のネットワークの接続についてのアクセス制御方針を定め、外部からの無権限アクセスを防止する。この作業は、守秘義務契約を結んだ第三者に委託することができる。

（アクセスログの採取と検査）

第 24 条　ネットワーク機器及びファイルサーバのシステム管理者は、アクセスログ採取及び検査についての方針を定め、アクセスログの採取及び検査を行う。この作業は、守秘義務契約を結んだ第三者に委託することができる。

（個人情報を用いたテストの禁止）

第 25 条　システム開発に関連し、システム開発テストを実施する場合、個人情報を用いてはならない。

（データのバックアップおよびリカバリーテストの実施）

第 26 条　システム管理者は、ファイルサーバに保管されているデータのバックアップ及びリカバリー方針を定めなければならない。

２　システム管理者は、ファイルサーバのデータバックアップを、方針に従い定期的に実施しなければならない。

３　システム管理者は、方針に従い定期的にリカバリーテストを実施しなければならない。

４　システム管理者は、リカバリーテストの結果を踏まえて、バックアップ及びリカバリー方針を変更しなければならない。

第 7 章 物理的・環境的対策

（セキュリティ区画の設定）

第 27 条　会社内の施設を、必要に応じ外部者が入室できる区画「応接室・会議室」と、事前に承認された者が入室できる区画「執務室」に区分する。

（入室管理）

第 28 条　外部者が「応接室・会議室」に入室する場合は、社員が必ず同席する。

２　外部者がレベル「執務室」に入室する場合は、社員が必ず同伴し、社員の指示に従い行動してもらうように依頼する。

（キャビネット、コンピュータ等の設置）

第 29 条　秘密文書を保管するキャビネットは、「執務室」に設置する。

２　ファイルサーバは、情報セキュリティー管理がその時点で自社管理のファイルサーバーで保たれるであろう情報セキュリティレベル以上のクラウドサーバーを活用する。バックアップコンピュータは「執務室」に設置し、代表取締役が管理する。

３　社内ネットワークは、すべてクラウドサーバーを介して行い、進入の危険のある自社のネットワーク機器は所持活用しない。

４　「応接室・会議室」にはネットワーク機器を設置しない。「執務室」には盗難又は外部者の事故等による破損を防止するために、施錠管理その他の適切な物理的対策を実施する。

第８章 教育・訓練

（教育・訓練）

第 30 条　情報セキュリティに関する教育を定期的に実施する。

２　技術的対策が確実に実施できるように、必要に応じ、訓練を実施する。

（教育・訓練の記録）

第 31 条　情報セキュリティに関する教育・訓練を実施した記録を保持する。

第９章 委託管理

（委託先の選定）

第 32 条　会社の業務を外部に委託する場合、委託先を選定するための条件として、委託先の情報管理についても考慮する。

２　外部委託先が反社会的勢力に属していないか、ネット検索（住所、氏名、生年月日による照会等）、誓約書の提出等で確認を行い、必要に応じて警察その他公的機関に問い合わせを行うことにより確認を行う。

（契約書の締結）

第 33 条　会社の業務を外部に委託する場合、委託先と業務委託契約を締結し、両者の責任の範囲及び実施する業務を明確にする。

２　契約書又はその覚書に次条の委託先に要求すべき情報セキュリティに関する事項を含めるように努める。

（委託先に要求すべき情報セキュリティに関する事項）

第 34 条　委託先に要求すべき情報セキュリティに関する事項として、以下の事項を要求する。

１）会社で要求している情報セキュリティに関する事項と同等の水準の遵守。

２）委託先の業務の遂行における情報セキュリティ関連事項について当社に対する定期的な報告を求める。

３）会社の職員又は会社が委託した者等が、委託先の業務の遂行における情報セキュリティ関連事項の遵守状況の報告をうけることにより確認を行う。

（委託先からの報告）

第 35 条　業務委託を行った部署の責任者は、業務の遂行におけるセキュリティ関連事項について、委託先から定期的な報告を受けなければならない。

２　必要に応じ、委託先との間で定期的な報告会を開催することが望ましい。

（委託先への確認）

第 36 条　業務委託を行った部署の責任者は、委託先の情報セキュリティ関連事項の契約事項の遵守状況を委託先から報告をうけることにより年に 1 度以上確認する。

２　前項の確認は、外部の専門家に委託することができる。

第１０章　事件・事故への対応

（事件・事故への対応）

第 37 条　クラウドファイルサーバのシステム管理者は、アクセスログの検査の結果、不正なアクセスを発見又はそのおそれを発見した者は、総務責任者及び契約しているシステム運用委託先に連絡しなければならない。

２　総務責任者は、システム管理者及びシステム運用委託先と相談し、対応を決めなければならない。

３　個人情報の漏えい事故の場合は、別途定める細則（独立行政法人情報処理推進機構セキュリティセンター作成【情報漏えい発生時の対応ポイント集】）に従い対応する。

４　個人情報の漏えい事故の場合は、懲戒の対象となり、対象行為における見解をまとめた上で、代表取締役の決定により以下の処分を行う。

1）口頭注意
2）譴責
3）減給
4）出勤停止
5）懲戒解雇

第１１章　情報セキュリティ実施状況の確認

（実施状況の確認と報告）

第 38 条　総務責任者は、情報セキュリティに関する規程等が遵守されていることを年に１度以上確認し、代表取締役に報告する。

２　情報セキュリティ実施状況の確認は、代表取締役自ら行うこと又は外部の専門家に委託することができる。

（委託先に要求すべき情報セキュリティに関する事項）

第 40 条　総務責任者は、実施状況の確認の結果、重大な問題が発見された場合は、代

表取締役に報告しなければならない。

（実施状況確認結果に基づく改善）

第 41 条　代表取締役は、必要に応じて情報セキュリティ実施状況確認の結果に基づく改善を指示しなければならない

附則

この基準は、2015 年 4 月 1 日からこれを施行する。